Strafrecht in der Finsternis: Zu dem Vorhaben eines „Darknet-Tatbestands“

Matthias Bäcker 2019-03-21T14:03:23

Am vergangenen Freitag hat der Bundesrat beschlossen, einen Gesetzentwurf einzubringen, durch den das Betreiben zugangsbeschränkter Handelsplattformen für illegale Waren und Dienstleistungen im Internet unter Strafe gestellt werden soll. Die neue Regelung soll es den Strafverfolgungsbehörden erleichtern, gegen kriminelle Machenschaften im sogenannten Darknet vorzugehen. Der Entwurf bestätigt eine bedenkliche Tendenz im IT-Strafrecht: Zunehmend werden gefährlich weite Regelungen geschaffen, deren praktischer Nutzen zweifelhaft ist.

Weitreichende Kriminalisierung internetbasierter Leistungen

Herzstück des Entwurfes ist ein neuer § 126a StGB, nach dem sich strafbar machen soll, wer „eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von [bestimmten] rechtswidrigen Taten zu ermöglichen oder zu fördern”. Auch wenn eine Ausschussempfehlung, die diesen Tatbestand noch ausdehnen wollte,im Bundesrat keine Mehrheit fand, handelt es sich um eine weit gefasste Norm mit unklaren Konturen.

Das Anbieten einer zugangsbeschränkten internetbasierten Leistung erfasst dem Wortlaut nach auch zahlreiche sozialadäquate Handlungen. Als „internetbasierte Leistung“ lässt sich jeder elektronische Kommunikationsdienst begreifen, der Daten über das Internet überträgt und bestimmten Personen einen Nutzen stiftet. Bezogen auf Anonymisierungsnetzwerke, denen der Gesetzentwurf primär gilt, lässt sich dieser Begriff neben den innerhalb eines solchen Netzwerks angebotenen Leistungen auch auf das Netzwerk selbst beziehen, das im OSI-Modell auf der (obersten) Anwendungsschicht des Internet verortet ist. Eine „internetbasierte Leistung“ erbringt danach etwa, wer einen Knoten des Tor-Netzwerks betreibt. Die mögliche Kriminalisierung von Anonymisierungs- und Verschlüsselungsdiensten durch § 126a StGB-E wurde dementsprechend bereits kritisiert.

Die weitere Voraussetzung, dass der Leistungszugang durch besondere technische Vorkehrungen beschränkt ist, entlässt Plattformen im allgemein zugänglichen Internet aus der Strafbarkeit, trägt aber ansonsten nicht dazu bei, den Tatbestand auf strafwürdige Handlungen zu beschränken. So nennt der Gesetzentwurf bereits die Nutzung eines Tor-Browsers als ausreichende Zugangsbeschränkung. Dabei handelt es sich nicht um ein arkanes kriminelles Werkzeug. Der Zugang zu Handelsplattformen im Darknet ist über Tor-Browser auch ohne nennenswerte IT-Kenntnisse möglich. Dies erkennt auch die Gesetzesbegründung an. Die

Handelsplattformen im Darknet böten „einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten."

Eine angemessene Eingrenzung der Strafbarkeit kann demnach nur die Voraussetzung liefern, dass Zweck oder Tätigkeit der Leistungen darauf ausgerichtet ist, die Begehung bestimmter rechtswidriger Taten zu ermöglichen oder zu fördern. Diese Formulierung ist an § 129 Abs. 1 Satz 1 StGB angelehnt. Diese Norm bedroht die Gründung von oder Beteiligung an Vereinigungen mit Strafe, deren Zwecke oder Tätigkeiten auf die Begehung von Straftaten gerichtet sind. Hier wird die Voraussetzung der Ausrichtung so interpretiert, dass die Begehung von Straftaten der verbindlich festgelegte Zweck einer Vereinigung sein und einfest gefasster Wille hierzu bestehen muss. Nur unter diesen Voraussetzungen ist nach der Rechtsprechung des Bundesgerichtshofs die Vorverlagerung der Strafbarkeit durch § 129 StGB gerechtfertigt. Ein bloßes Bewusstsein, dass es zu Straftaten kommen könnte, reicht nicht aus.

Es ist allerdings unklar, ob sich diese engen Voraussetzungen auf § 126a StGB-E übertragen lassen. Denn dieser verlangt im Unterschied zu § 129 StGB nicht, dass die internetbasierte Leistung auf die *Begehung* von Straftaten ausgerichtet ist, sondern lediglich auf deren *Ermöglichung* oder *Förderung*. Der Anbieter muss also gerade nicht bezwecken, dass mithilfe seiner Plattform tatsächlich Straftaten begangen werden. Er muss lediglich zweckgerichtet ein Umfeld schaffen, in dem solche Straftaten naheliegen. Diese subtile Unterscheidung könnte sich als entscheidende Weichenstellung erweisen. Anbieter internetbasierter Leistungen könnten sich demnach schon wegen der von ihnen erkannten objektiven Eignung ihrer Angebote strafbar machen, kriminelles Verhalten zu fördern. Praktisch ist zu befürchten, dass eine solche objektive Affinität bei nahezu allen Diensten angenommen werden könnte, die über das Tor-Netzwerk erreichbar sind oder die dieses Netzwerk bereitstellen. Immerhin kam eine empirische Studie im Jahr 2016 zu dem Ergebnis, dass über die Hälfte der untersuchten Websites im Tor-Netzwerk illegale Angebote enthielten.

Die Begründung des Entwurfes liefert im Übrigen keine klaren Anhaltspunkte dafür, was die Ausrichtung zur Ermöglichung und Förderung von Straftaten erfordert und räumt der Praxis einen weiten Interpretationsspielraum ein. Die Prüfung habe „anhand des konkreten Einzelfalls zu erfolgen" und sei „allgemein verbindlichen Kriterien nicht zugänglich". Die Ausrichtung von Plattformen solle nach Indizien wie ihrem tatsächlichen Angebot, dem Umgang mit Hinweisen auf illegale Aktivitäten und den Vorgaben in ihren AGB festgestellt werden. Gerade der Gedanke, die Prüfung der AGB einer Darknet-Plattform könne zur Einordnung ihrer kriminellen Ausrichtung beitragen, erscheint allerdings wenig realitätsnah.

Vorverlagerung und strafrechtliche „Störerhaftung"

Durch seine weite Fassung soll der Straftatbestand laut der Entwurfsbegründung praktischen Problemen begegnen, Plattformbetreiber wegen Beihilfe (§ 27 StGB)

zu Straftaten zu bestrafen, die über die Plattform begangen werden. Die Beihilfe sei oft nicht nachweisbar, „da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle abgewickelt werden“. Zudem seien bei „vielen Foren die Arten von Straftaten, die über sie abgewickelt werden sollen, zu Beginn nicht klar definiert.“ Es lässt sich allerdings darüber streiten, ob dies dem Vorliegen einer strafbaren Beihilfe entgegensteht. Der Bundesgerichtshof stellt besonders an den Vorsatz eines Gehilfen geringe Anforderungen und lässt es schon ausreichen, dass er „dem Täter ein entscheidendes Tatmittel willentlich an die Hand gibt und damit bewusst das Risiko erhöht, dass eine durch den Einsatz gerade dieses Mittels geförderte Haupttat verübt wird“. Wenn eine Plattform gezielt als Umschlagplatz für kriminelle Geschäfte konzipiert ist und sich eine Straftat nachweisen lässt, die über die Plattform abgewickelt wurde, wird darum zumindest eine Beihilfestrafbarkeit des Plattformbetreibers in aller Regel feststehen. Bei manchen Transaktionsstraftaten wie dem Handeltreiben mit Betäubungsmitteln oder Waffen kann das Vermitteln illegaler Transaktionen sogar bereits eine eigenständige täterschaftliche Tatbegehung darstellen.

Unabhängig davon geht § 126a StGB-E tatbestandlich weit darüber hinaus, Nachweisprobleme bei der Beihilfe zu beseitigen. Der vorgeschlagene Tatbestand führt zu einer massiven Vorverlagerung der Strafbarkeit, wie auch seine Nähe zu § 129 StGB zeigt. Das Anbieten der genannten internetbasierten Leistungen ist nach der geplanten Regelung unabhängig davon strafbar, ob eine rechtswidrige Haupttat überhaupt vorliegt. Es dürfte beispielsweise ausreichen, ein Diskussionsforum oder eine Vertriebsplattform mit einer hinreichenden Affinität zur Förderung von Straftaten im Darknet zu eröffnen, um den Tatbestand zu erfüllen. Der Betreiber und seine Unterstützer (wie etwa technische Dienstleister) könnten schon strafbar sein, bevor überhaupt ein kriminelles Geschäft über die Plattform geplant oder abgewickelt worden wäre oder sich auch nur jemand dort angemeldet hätte.

Eher als Nachweisprobleme bei der Beihilfe zu beseitigen, begründet § 126a StGB-E damit eine im IT-Strafrecht bisher beispiellose Vorfeldstrafbarkeit. In diese Richtung deutet auch die Behauptung der Begründung, dass „die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind“. Diese Aussage ist angesichts des weiten Wortlauts und der weiten Auslegung von § 27 Abs. 1 StGB durch die Rechtsprechung einigermaßen erstaunlich, wenn sie auf bereits begangene Haupttaten bezogen wird. Sie ergibt aber Sinn, wenn die Strafbarkeit der Tatbegehung zuvorkommen soll.

Die weitere Feststellung der Gesetzesbegründung, dass Personen, die „nur für die Aufrechterhaltung und Wartung der technischen Infrastruktur oder die Administration nicht strafrechtlich relevanter Bereiche zuständig sind und glaubhaft versichern, keine Kenntnis von oder jedenfalls kein Interesse an den über das Forum abgeschlossenen oder angebahnten illegalen Verkaufstätigkeiten gehabt zu haben“, nicht wegen Beihilfe bestraft werden können, mag zutreffen. Allerdings ist auch zweifelhaft, ob sich solche Personen generell strafwürdig verhalten. Fragwürdig erscheint dies insbesondere, wenn eine größere Plattform wie ein Diskussionsforum oder eine Verkaufsbörse neben einzelnen strafrechtlich relevanten

Segmenten primär legale Nutzungen ermöglicht. Wer sich an einer solchen Plattform technisch oder administrativ beteiligt und hinsichtlich der strafbaren Nutzungen lediglich mit Eventualvorsatz handelt, verhält sich kaum anders als viele Beschäftigte in herkömmlichen Wirtschaftszweigen, deren Verhalten gemeinhin als völlig legal angesehen wird. So käme wohl niemand auf die Idee, eine in einer Großkanzlei tätige Rechtsanwältin allein deshalb bestrafen zu wollen, weil sie an der Geschäftstätigkeit der Kanzlei mitwirkt und ihr bewusst ist, dass Kolleginnen und Kollegen in anderen Abteilungen an anderen Standorten und im Rahmen anderer Mandate zu Steuerhinterziehungen oder Geldwäschedelikten beitragen. Für leitende Angestellte in der Industrie ließen sich ähnliche Szenarien entwerfen. In diesem Zusammenhang ist zu berücksichtigen, dass Dienste wie das Tor-Netzwerk keineswegs nur zu kriminellen Zwecken genutzt werden, sondern auch sozial wünschenswerte Tätigkeiten ermöglichen – etwa im journalistischen oder humanitären Bereich.

Im Ergebnis führt § 126a StGB-E somit zu einer strafrechtlichen „Störerhaftung“, die primär den präventiven Zweck verfolgt, kriminelle Geschäftsmodelle im Darknet gar nicht erst entstehen zu lassen. Eine Würdigung des individuellen Verhaltens der handelnden Einzelpersonen wird demgegenüber weitgehend entbehrlich. Zu diesem Verständnis der geplanten Regelung passt einerseits die systematische Stellung im Rahmen der Straftaten gegen die öffentliche Ordnung (§§ 123 ff. StGB), andererseits die in der Entwurfsbegründung immer wieder vorgetragene Auffassung, dass Handelsplattformen im Darknet als Gefahr für die öffentliche Sicherheit anzusehen seien.

Neben der Strafbarkeit verlagert der geplante Straftatbestand schließlich auch den Anwendungsbereich der Ermittlungsermächtigungen des Strafprozessrechts vor. Aufgrund der Weite des Tatbestands wird sich ein Anfangsverdacht leicht annehmen lassen. Zudem soll das Anbieten von Leistungen zur Ermöglichung von Straftaten zukünftig im Falle seiner gewerbsmäßigen Begehung (§ 126a Abs. 3 StGB-E) auch die Möglichkeit zu Telekommunikationsüberwachungen eröffnen. Hierzu soll die Überwachungsermächtigung des § 100a StPO erweitert werden. Der für die Gewerbsmäßigkeit erforderliche Wille, sich durch wiederholtes Handeln eine fortlaufende Einnahmequelle von einiger Dauer und einigem Umfang zu verschaffen, wird bei den Anbietern internetbasierter Dienste regelmäßig vorliegen. Selbst wenn letztlich strafrechtliche Verurteilungen nach § 126a StGB-E selten bleiben sollten, könnte diese Ermittlungsfunktion des geplanten Tatbestands – wie häufig im strafrechtlichen Vorfeldrecht – praktisch erhebliche Bedeutung erlangen.

Vereinbarkeit mit höherrangigem Recht

Die weite Fassung des geplanten Straftatbestands und die potenzielle Kriminalisierung zahlreicher Anbieter von internetbasierten Dienstleistungen werfen die Frage auf, wie der Entwurf verfassungsrechtlich zu bewerten ist. Verletzt sein könnten sowohl das strafrechtliche Bestimmtheitsgebot (Art. 103 Abs. 2 GG) als auch die Grundrechte der Anbieterinnen insbesondere von gesellschaftlich nützlichen Leistungen wie etwa Anonymisierungsdiensten (Art. 12 Abs. 1 GG). Allerdings verfolgt das Bundesverfassungsgericht bei der Beurteilung strafrechtlicher

Normen, selbst wenn sie vage formuliert sind oder ihr Ziel zweifelhaft erscheint, gegenüber dem Gesetzgeber seit langem eine sehr permissive Linie. Danach dürfte es Aufgabe der Strafverfolgungsbehörden und der Strafgerichte sein, die überschießenden Tendenzen des geplanten Tatbestands bei dessen Auslegung und Anwendung zu bewältigen. Abzuwarten ist, ob hier die für dieses Jahr angekündigte Entscheidung über die Verfassungsbeschwerde gegen den Straftatbestand der „Datenhehlerei“ (1 BvR 2821/16) zu neuen Erkenntnissen führen wird. Ähnlich wie § 126a StGB-E war auch § 202d StGB mit dem Ziel angetreten, Strafbarkeitslücken für den Handel über Plattformen im Darknet zu schließen, schoss aber in seiner Weite deutlich über das Ziel hinaus.

Wirksamere Grenzen für die präventive Indienstnahme des Strafrechts gegenüber den Anbietern internetbasierter Leistungen könnten sich aus dem Unionsrecht ergeben. Insbesondere stellt sich die Frage, ob der Entwurf nicht die von der E-Commerce-Richtlinie vorgegebenen und durch §§ 7 ff. TMG in deutsches Recht umgesetzten Haftungsprivilegien von Host- und Access-Providern aushebelt. Danach sind Provider nur unter qualifizierten Voraussetzungen für die von ihnen übermittelten oder gespeicherten Inhalte verantwortlich. Hingegen begründet § 126a StGB-E zumindest bei weiter Auslegung eine sehr weitreichende strafrechtliche Providerhaftung. Wie dieses Spannungsverhältnis aufzulösen ist, lässt der Entwurf im Dunkeln. Die Entwurfsbegründung erwähnt die Haftungsprivilegierungen des Telemedienrechts nicht einmal. Sie könnten jedoch wegen des Anwendungsvorrangs der E-Commerce-Richtlinie in der Praxis zur Folge haben, dass von der intendierten Vorverlagerung der Strafbarkeit im Ergebnis wenig übrigbleibt.

Fazit

Der Entwurf eines „Darknet-Tatbestandes“ fügt sich in einen allgemeinen Trend ein, das Strafrecht präventiv in Dienst zu nehmen, um kriminelle Bedrohungen möglichst schon im Keim zu ersticken. Neben den bereits klassischen Referenzfeldern des Terrorismus und der (herkömmlichen) organisierten Kriminalität zeigt sich dieser Trend gerade auch im IT-Strafrecht mittlerweile besonders deutlich, wie etwa der misslungene Tatbestand der Datenhehlerei (§ 202d StGB) und das Vorhaben einer ausufernden Strafbarkeit für den „digitalen Hausfriedensbruch“ belegen. Die präventive Nutzung des Strafrechts bringt extrem weit gefasste Deliktstatbestände mit sich, die erst im Prozess der Rechtsanwendung (hoffentlich) Konturen gewinnen werden – falls es denn überhaupt zu hinreichend vielen Verfahren kommt. Wird der Entwurf verabschiedet, entstehen zumindest auf absehbare Zeit für die Anbieter sozial wünschenswerter internetbasierter Leistungen beträchtliche Strafbarkeitsrisiken. Diese Risiken schaffen nicht nur individuelle Bedrängnisse, sondern können zudem technische und soziale Innovationen hemmen. Ob das Ziel einer möglichst lückenlosen Kriminalisierung derjenigen, die sich an kriminellen Transaktionen im Darknet beteiligen, den Preis solcher Kollateralschäden wert ist, erscheint höchst fragwürdig. Gerade wenn es um freiheitssichernde Angebote wie Verschlüsselungs- und Anonymisierungsdienste geht, sollte die Expansion des Strafrechts mit mehr Fingerspitzengefühl betrieben werden.